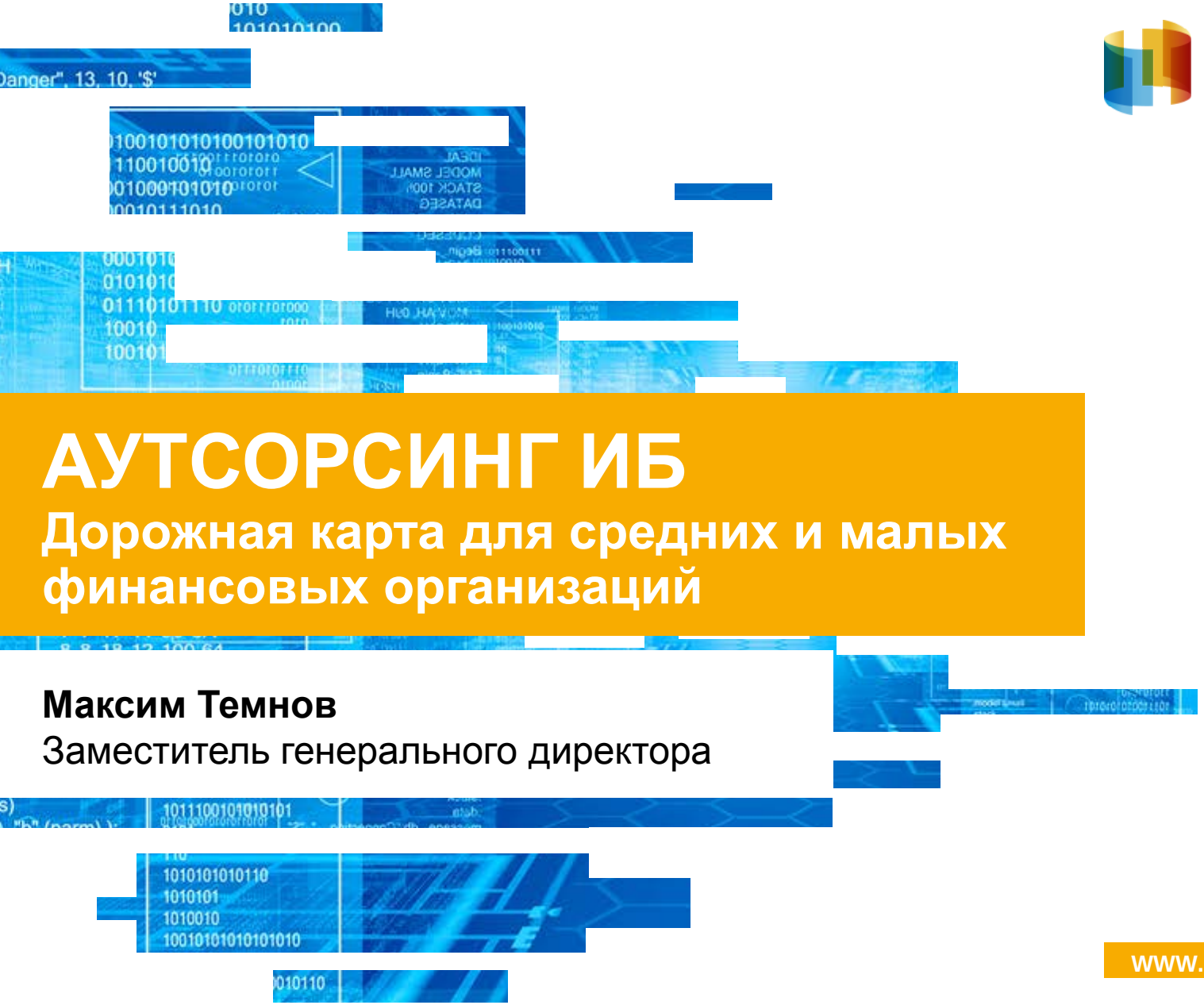


Информзащита
Системный интегратор

АУТСОРСИНГ ИБ

Дорожная карта для средних и малых финансовых организаций

Максим Темнов
Заместитель генерального директора

Информзащита
Системный интегратор

АУТСОРИНГ ИБ
Взгляд регулятора

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ АУТСОРСИНГА ИБ

WWW.INFOSEC.RU

НОРМАТИВЫ ДЛЯ БАНКОВ

Норматив	Область регулирования	Регулятор	Способы контроля	Приоритет для Банка
382-П	Безопасность безналичных платежей	ЦБ РФ	1 раз в 2 года отчет в ЦБ	Важно
552-П	Подключение к ЦБ РФ АРМ КБР, АРМ ПУР	ЦБ РФ	1 раз в квартал оформлять отчет	Важно
152-ФЗ (ПДн)	Безопасность обработки персональных данных (ПДн)	Роскомнадзор	Периодические проверки Роскомнадзора	Средне или важно
PCI DSS	Безопасность данных платежных карт	МПС (Visa, Mastercard и др.)	1 раз в год отчет в МПС (Visa/Mastercard)	Важно, если есть процессинг или требует банк, спонсирующий участие в МПС
СТО БР	Обеспечение ИБ технологических процессов обработки платежной и неплатежной информации	ЦБ РФ	1 раз в 2 года отчет в ЦБ	Важно – если в банке сильные позиции ИБ и СТО БР введен как обязательный.
SWIFT Customer Security Programme (CSP)	Обеспечение безопасности переводов через SWIFT	SWIFT	Отчет в SWIFT 1 раз в год	2017 год – средне, 2018 год – важно
242-П	Организация внутреннего контроля и тестирование планов ОНиВД	ЦБ РФ	Во время проверки ЦБ может запросить информацию о проведении тестирований плана ОНиВД	Данных нет
397-П	Ведение электронных баз данных	ЦБ РФ	ЦБ может запросить базу за любую дату, банк обязан предоставить в 3 дня	Данных нет
187-ФЗ (КИИ)	Безопасности критической информационной инфраструктуры РФ	ФСТЭК, ФСБ, ЦБ, Минкомсвязь	Периодический аудит	Средне или важно
ГОСТ Р 57580.1—2017	Обеспечение ИБ технологических процессов обработки платежной и неплатежной информации	ЦБ	Периодический аудит	Средне или важно

ЦБ: РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ
Обеспечение информационной безопасности организаций банковской системы российской федерации
АУТСОРСИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОДХОДЫ К АУТСОРСИНГУ ИБ

Кратковременное сотрудничество

Усиление СОИБ услугами аутсорсинга на время проведения крупных мероприятий, характерных увеличением рисков ИБ (например, политические саммиты, выборы, спортивные соревнования, международные конкурсы и другое).

Среднесрочное сотрудничество

На аутсорсинг временно передаются сложные технологические процессы СОИБ до тех пор, пока не будет реализован соответствующий процесс внутри организации БС РФ. Например, процесс мониторинга событий ИБ может быть передан на аутсорсинг на время построения собственного Центра мониторинга и реагирования.

Долговременное сотрудничество

На аутсорсинг передаются непрофильные и/или сложные процессы ИБ (например, мониторинг событий и реагирование на инциденты ИБ).

ОСНОВНЫЕ ПРИЧИНЫ ИСПОЛЬЗОВАНИЯ АУТСОРСИНГА ИБ

Кадровые

- Отсутствие необходимых квалифицированных и мотивированных кадров внутри организации БС РФ;
- Необходимость высвобождения ключевых специалистов для других проектов и задач;
- Необходимость снижения зависимости от собственных работников организации БС РФ

Экономические

- Повышение прозрачности и предсказуемости расходов на СОИБ;
- Оптимизация расходов на СОИБ;

Технологические

- Повышение общего уровня ИБ за счет использования современных технологий и методологий;
- Возможность обеспечения отдельных процессов СОИБ в режиме 24x7;

Временные

- Возможность быстрого внедрения отдельных процессов СОИБ;
- Возможность быстрого повышения уровня зрелости отдельных процессов СОИБ.

ВОЗМОЖНЫЕ УСЛУГИ АУТСОРСИНГА ИБ

Средним и малым организациям БС РФ в первую очередь следует ориентироваться на следующие:

- Мониторинг и анализ событий информационной безопасности для критичных систем;
- Выявление атак на критичные информационные системы (в том числе с использованием информации, получаемой от Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT));
- Анализ защищенности (управление сканерами уязвимостей);
- Контроль конфигураций сетевого оборудования и операционных систем;
- Управление IDS/IPS;
- Анализ безопасности кода приложений;
- Предоставление и администрирование WAF;
- Обучение и повышение осведомленности персонала.

«Для многих небольших и средних банков вопросы, связанные с кибербезопасностью и IT в целом, весьма недешевые и сложные. Здесь вполне возможны варианты использования аутсорсинга».

Артем Сычев, «Известия» от 28.07.2017

Информзащита
Системный интегратор

АУТСОРСИНГ ИБ
Взгляд поставщика услуг

ПРЕДЛОЖЕНИЕ ДЛЯ СМБ – БАНКОВ

WWW.INFOSEC.RU

ПРОБЛЕМАТИКА

Что мешает СМБ - банку соответствовать требованиям?

Информзащита
Системный интегратор

- Техническая проблема: отсутствие части технических средств и организационных мер по защите информации соответствующего класса.
- Отсутствие квалифицированного персонала не позволяет внедрить технические средства и выстроить процессы обеспечения информационной безопасности.
- Большинство предложений на рынке информационной безопасности не предлагают комплексный подход по закрытию требований и реальную безопасность , делая акцент на конкретные подсистемы безопасности и «лоскутность». .
- Оптимизация бюджетов приводит к экономии на безопасности.

Необходимы инвестиции в технические средства и квалифицированный персонал для закрытия всех требований регуляторов

РЕШЕНИЕ ОТ ПОСТАВЩИКА

Услуга аутсорсинга ИБ

Информзащита
Системный интегратор

опыт и экспертиза

compliance

стенды

проверка эффективности

комплексный анализ требований регуляторов

ТИПОВЫЕ РЕШЕНИЯ

ДЛЯ РЕАЛЬНОЙ БЕЗОПАСНОСТИ

тестирование

необходимые технические средства

понимание потребностей банков

высококвалифицированные эксперты

РЕАЛИЗАЦИЯ УСЛУГИ

Информзащита
Системный интегратор

Услуга представлена в виде трех пакетов:

Пакет «Минимальный»	• обеспечивает соответствия требованиям регуляторов используя совместно коммерческие продукты и решения Open Source
Пакет «Эконом»	• сбалансированный вариант: обеспечивает соответствия требованиям регуляторов сертифицированными решениями с минимальным функционалом и стоимостью
Пакет «Оптимальный»	• обеспечивает соответствия требованиям регуляторов сертифицированными решениями корпоративного уровня с оптимальным уровнем защиты

СОСТАВ УСЛУГИ

Информзащита
Системный интегратор

1. Проведение аудита и анализа СОИБ

2. Доработка базового технического решения:

- формирование спецификации на ПАК

3. Формирование комплекта документов под Заказчика:

- формирование базового комплекта ОРД
- доработка эксплуатационной документации

4. Внедрение СЗИ:

- установка и настройка
- опытно-промышленная эксплуатация

Межсетевой экран
IDS\IPS
Антивирус
СКЗИ
СЗИ от НСД

СЗИ от НСД
Сканер уязвимостей
Защита виртуализации
Средства мониторинга ИБ

5. Сопровождение в процессе эксплуатации

- техническая поддержка и сопровождение СЗИ
- работа с событиями ИБ

ПОЧЕМУ АУТСОРСИНГ ?

Информзащита
Системный интегратор

Традиционная модель	VS	Аутсорсинг

Основной документ

Трудовой договор с профильными специалистами в области ИБ

SLA (Service Level Agreement) – Соглашение об уровне сервиса

Уровень ответственности

Выполнение работ в рамках должностных инструкций:
- Скорость и качество выполнения функциональных задач;
- Персональная ответственность за каждую задачу.

Работоспособность обслуживаемой ИБ-системы:
- Скорость и качество выполнения функций по эксплуатации;
- Обеспечение параметров надежности и доступности (SLA).

Финансовая составляющая

- Формирование, контроль и корректировка бюджетов на каждый проект.
- Бюджет закупки, внедрения, ФОТ (ЗП, бэк-офис, и т.д.), ТП производителя.

- Прогнозируемость расходов (фиксированная стоимость).
- Размер оплаты зависит от объема и качества предоставляемых услуг.

1. Аудит и документация:
- **(382-П) - ~900 тыс. руб.**
- **(552-П) - ~500 тыс. руб.**
- **(152-ФЗ) - ~800 тыс. руб.**

2. Поставка и внедрение СЗИ:
- **2 500 тыс. руб. – 7 000 тыс. руб.**

3. Эксплуатация СЗИ:
~4 350 тыс. руб.* *(*ФОТ 2-х специалистов)*

от 9 050 тыс. руб.
до 13 550 тыс. руб.

1. Аудит и документация
2. Поставка и внедрение СЗИ
3. Эксплуатация СЗИ

от 4 000 тыс. руб.
до 10 500 тыс. руб.

В зависимости от задач доступны специалисты нужного уровня и квалификации

КОМПЛЕКСНЫЙ ПОДХОД

Информзащита
Системный интегратор

СЗИ

- Поставка
- Внедрение
- Техническая поддержка

КОНСАЛТИНГ

- Проверка соответствия требованиям регуляторов
- Пакет документов
- Экспресс-аудиты безопасности

ОТЧЕТНОСТЬ

- Отчетность по требованиям регуляторов
- Отчетность по состоянию ИБ

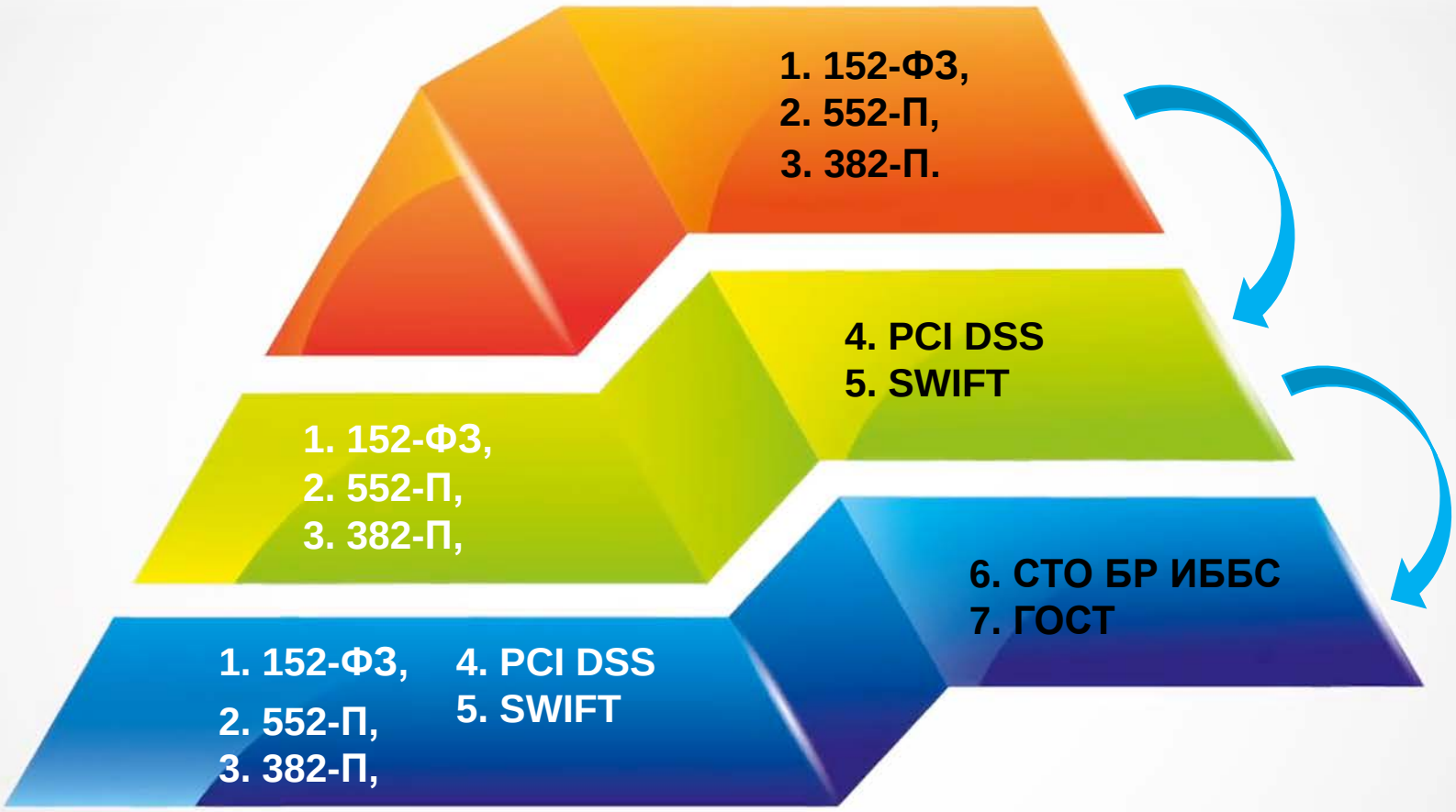
ОБЕСПЕЧЕНИЕ ИБ

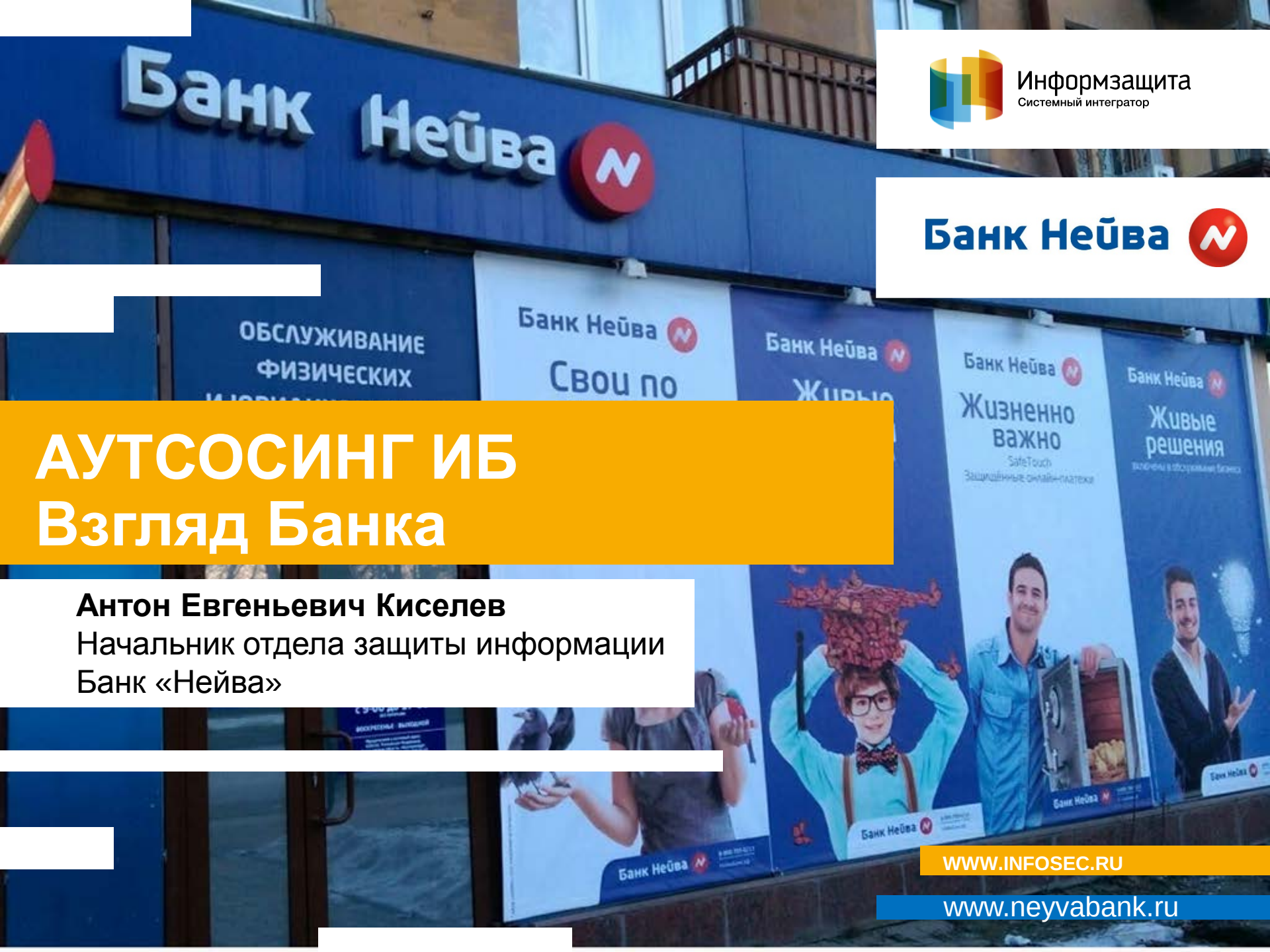
- Мониторинг событий ИБ
- Сканирование и меры по устранению уязвимостей

ПРОСТО. ЭФФЕКТИВНО. ОПТИМАЛЬНО.

ЭТАПЫ ПРОРАБОТКИ ВОПРОСА

Информзащита
Системный интегратор





Информзащита
Системный интегратор

Банк Нейва

АУТСОСИНГ ИБ
Взгляд Банка

Антон Евгеньевич Киселев
Начальник отдела защиты информации
Банк «Нейва»

WWW.INFOSEC.RU

www.neyvabank.ru

РИСКИ СВЯЗАННЫЕ С ИБ

Банк Нейва

Правовые

Риски нарушение законодательства:

- Нарушение требований уголовного и административного законодательства;
- Нарушение требований регуляторов.

Операционные

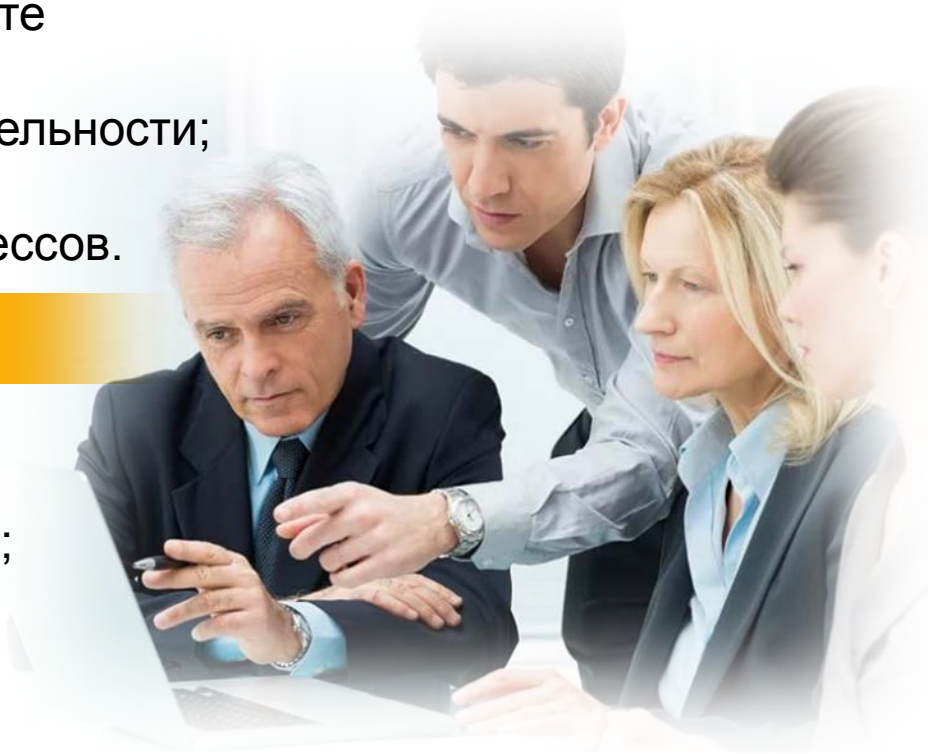
Риск возникновения убытков в результате инцидентов ИБ:

- Прерывание операционной деятельности;
- Кража денежных средств;
- Нарушение работы бизнес процессов.

Репутационные

Риск потери деловой репутации перед клиентами Банка:

- Потеря потенциальных клиентов;
- Отток текущих клиентов.



КОНФЛИКТ ИНТЕРЕСОВ В ПРОЦЕССЕ АУТСОРСИНГА

Банк Нейва

Интересы Заказчика:
- Минимальный бюджет
- Максимум работ

КОНФЛИКТ

Интересы Исполнителя:
- Максимальный бюджет
- Минимум работ

Практика решения в аутсорсинге:

- Подробное описание каталога услуг;
- Прозрачное ценообразование;
- Четкий SLA;
- Контроль качества по KPI
- Подписанный NDA;
- Оплата по фиксированному объему оказанных услуг.

АУТСОРСИНГ. ЗАЧЕМ?

Банк Нейва

Каждый банк пытается своими силами выполнить одно и тоже

при этом

Угрозы ИБ однотипные

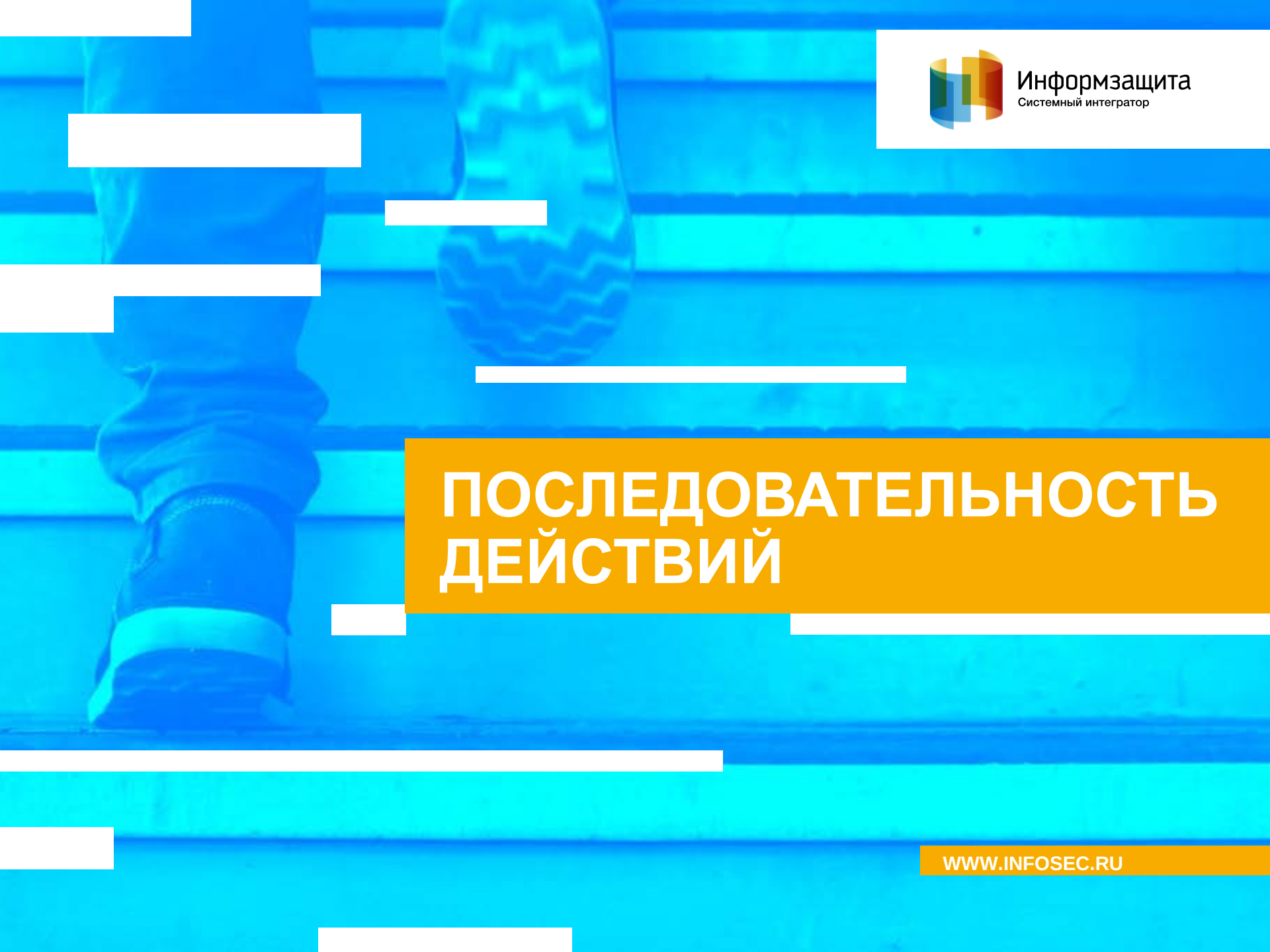
Требования по ИБ к банкам единые

Решения по защите информации типовые

Разумно не разрабатывать все самостоятельно, а воспользоваться готовым решением и кастомизировать его под свои нужды.

Пример:
Самостоятельное приведение Банка в соответствие требованиям 382-П заняло **1,5** человека-года.

Аутсорсер выполняет за **3** месяца



Информзащита
Системный интегратор

ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ

WWW.INFOSEC.RU

ЧТО ДАЛЬШЕ?
(road map)

Информзащита
Системный интегратор

Этап №1

- Экспресс-оценка текущего уровня безопасности
- Внедрение базового решения по обеспечению ИБ

Этап №2

- Подключение к FinCert через Коммерческий SOC

Этап №3

- Экспертная помощь при кибератаках

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 24x7x365

«ИНФОРМЗАЩИТА»:

- **СИСТЕМНЫЙ ИНТЕГРАТОР WWW.INFOSEC.RU**
- **СЕРВИСНЫЙ ЦЕНТР WWW.ITSOC.RU**
- **УЧЕБНЫЙ ЦЕНТР WWW.ITSECURITY.RU**